Amendment to the Claims:

This listing of claims replaces all prior versions, and listings, of claims in the application:

1-16 (Canceled).

17. (Currently Amended) A network system, comprising:

first and second devices, wherein the first device is adapted to:

deliver a set of policies to the second device during initialization of a virtual private network between the first and second devices;

and the second device is adapted to:

run an application;

use both said policies and a priority assigned to the ~~state of said~~ application to detect data packets from unauthorized activities; and

reject data packets from the unauthorized activities.

18. (Original) The system of claim 17 further comprising a network stack.

19. (Original) The system of claim 18, wherein the network stack comprises:

a policy engine connected to the first device;

a policy store connected to the policy engine;

a socket interceptor connected to the policy engine; and

a packet guard connected to the policy engine.

20. (Original) The system of claim 17, the first device further comprising instructions to monitor the system for the intervening processes.

21. (Currently Amended) A network stack, comprising:

a policy engine;

a policy store adapted to interact with the policy engine and store a set of policies from the policy engine;

a socket interceptor coupled to the policy engine;

a packet guard coupled to the policy engine;

a configurable management process adapted to reconfigure the network stack and having instructions to:

receive policies in the policy engine from the policy server during a virtual private network session;

use the socket interceptor to detect and reject data packets from unauthorized users and applications and provide the packet guard with context information about the

unauthorized users and applications including at least information a priority ~~about a running state~~ of the application;

use the packet guard to filter unauthorized activities received from the network interface;

use the packet guard to filter the data packets from unauthorized users and applications based on the context information received by the socket interceptor; and

use the packet guard to filter data packets based on the policies.

22. (Original) The network stack of claim 21 further comprising a packet translator adapted to interact with the socket interceptor and the packet guard.

23. (Original) The network stack of claim 21 further comprising an interface to a network adapted to connect the network stack to the network, wherein the network has a policy server.

24-28. (Canceled)

29. (Previously Presented) A system as in claim 17, wherein said second device uses said policies to determine if an

application is running and allows certain kinds of network packets, associated with said network application, to pass only when said application is running and to be blocked when said application is not running.

30. (Currently Amended) A method~~,~~ comprising:

establishing a virtual private network (VPN) session between a primary computing system and a remote computing system, wherein the primary computing system includes a security policy engine, and wherein the remote computing system includes a network stack;

transmitting information indicative of security parameters from the primary computing system to the remote computing system using the security policy engine during initialization of the VPN;

configuring the network stack based on the information indicative of security parameters;

subsequently running a particular application program on the remote computing system;

selecting information indicative of updated security parameters based on a priority ~~running state~~ of the particular application program; and

dynamically reconfiguring the network stack based on the information indicative of the updated security parameters.

31. (Previously Presented) The method of claim 30, wherein the primary computing system is a corporate local area network (LAN).

32. (Previously Presented) The method of claim 30, wherein the remote primary computing system is a remote home network.

33. (Currently Amended) The method of claim 30, wherein the particular application program is a word processing program, and wherein, when a ~~the~~ running state of the word processing program indicates that the word processing program is not running, the information indicative of security parameters causes the remote computing system to block word processing packets received at the remote computing system.

34. (Currently Amended) The method of claim 30, wherein the particular application program is a word processing program, and wherein, when a ~~the~~ running state of the word processing program indicates that the word processing program is running, the information indicative of updated security parameters causes the remote computing system to not block word processing packets received at the remote computing system.

35. (New) A method comprising:

establishing a secure virtual private network connection between a server and a remote system;

delivering security policies from the server to the remote system during initialization of the secure private network connection; and

regulating access to nodes accessible via the server by the remote system based on the security policies and a priority associated with at least one application program running on the remote system.

36. (New) The method of claim 35 wherein regulating access comprises providing filters that are adapted to reject unauthorized data packets based on rejection criteria that are conditioned on the security policies and the priority of the at least one application program.

37. (New) The method of claim 35 wherein regulating access comprises:

providing a session layer adapted to reject unauthorized data packets based on context information; and

providing filters adapted to reject unauthorized data packets based on rejection criteria from at least one of the context information and the policies.

38. (New) The method of claim 35 further comprising updating the set of policies.

39. (New) The method as in claim 35, wherein the remote system includes a network stack, and wherein the regulating access comprises reconfiguring the network stack to control filtering of network packets, based on the policies and the priority of the application.

40. (New) The method as in claim 35, wherein the policies include information about authorized kinds of information when certain applications are running, and regulating access comprises determining if a specified application is running, allowing a specified kind of network packet to pass only when the specified application is running, and blocking the specified kind of network packet from passing when the specified application is not running.

41. (New) The method as in claim 40, wherein the specified application is a word processing program, and the kind of network packet is word processing data.

42. (New) An article comprising a computer-readable medium which stores computer-executable instructions, the instructions causing a computer to:

establish a secure virtual private network connection between a server and a remote system;

deliver security policies from the server to the remote system during initialization of the secure private network connection; and

regulate access to nodes accessible via the server by the remote system based on the security policies and a priority associated with at least one application program running on the remote system.

43. (New) The article of claim 42 wherein regulating access comprises providing filters that are adapted to reject unauthorized data packets based on rejection criteria that are conditioned on the security policies and the priority of the at least one application program.

44. (New) The article of claim 42 wherein regulating access comprises:

providing a session layer adapted to reject unauthorized data packets based on context information; and

providing filters adapted to reject unauthorized data packets based on rejection criteria from at least one of the context information and the policies.

45. (New) The article of claim 42 further comprising updating the set of policies.

46. (New) The article as in claim 42, wherein the policies include information about authorized kinds of information when certain applications are running, and regulating access comprises determining if a specified application is running, and allowing a specified kind of network packet to pass only when the specified application is running, based on the policies, and, blocking the specified kind of network packet from passing, when the specified application is not running, based on the policies.